10/524654 #2
PCT/EP03/50386

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

22 09 2003

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 02 SEP. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livreVI

REQUÊTE EN DÉLIVRANCE

DATE DE REMISE DES PIÈCES: 21 août 2002 N° D'ENREGISTREMENT NATIONAL: 0210430 DÉPARTEMENT DE DÉPÔT: 75 DATE DE DÉPÔT: 21 AOUT 2002	Karine BERTHIER THOMSON multimedia 46 Quai Alphonse Le Gallo 92648 Boulogne cedex France
Vos références pour ce dossier: PF020104	

1 NATURE DE LA DEMANDE			
Demande de brevet			
2 TITRE DE L'INVENTION			
	APPAREIL ELECTRIQUE SECURISE CONTRE LE VOL, SYSTEME ANTIVOL COMPORTANT UN TEL APPAREIL ET PROCEDE D'APPARIEMENT D'APPAREILS ELECTRIQUES		
3 DECLARATION DE PRIORITE OU REQUETE DU BENEFICE DE LA DATE DE DEPOT D'UNE DEMANDE ANTERIEURE FRANCAISE	Pays ou organisation	Date	N°
4-1 DEMANDEUR			
Nom	THOMSON LICENSING S.A.		
Suivi par	Karine BERTHIER		
Rue	46 Quai Alphonse Le Gallo		
Code postal et ville	92100 BOULOGNE-BILLANCOURT		
Pays	France		
Nationalité	France		
Forme juridique	Société anonyme		
N° SIREN	383 461 191		
Code APE-NAF	322A		
N° de téléphone	01 41 86 50 00		
N° de télécopie	01 41 86 56 34		
Courrier électronique	berthierk@thmulti.com		
5A MANDATAIRE			
Nom	BERTHIER		
Prénom	Karine		
Qualité	Liste spéciale, Pouvoir général: 9016		
Cabinet ou Société	THOMSON multimedia		
Rue	46 Quai Alphonse Le Gallo		
Code postal et ville	92648 Boulogne cedex		
N° de téléphone	01 41 86 54 88		
N° de télécopie	01 41 86 56 33		
Courrier électronique	berthierk@thmulti.com		

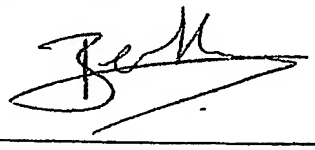
6 DOCUMENTS ET FICHIERS JOINTS	Fichier électronique	Pages	Détails
Description	desc.pdf	9	
Revendications	V	4	20
Dessins		2	3 fig., 3 ex.
Abrégé	V	1	
Désignation d'inventeurs			
Listage des sequences, PDF			
Rapport de recherche			

7 MODE DE PAIEMENT	
Mode de paiement	Prélèvement du compte courant
Numéro du compte client	626
Remboursement à effectuer sur le compte n°	626

8 RAPPORT DE RECHERCHE	
Etablissement immédiat	

9 REDEVANCES JOINTES	Devise	Taux	Quantité	Montant à payer
062 Dépôt	EURO	35.00	1.00	35.00
063 Rapport de recherche (R.R.)	EURO	320.00	1.00	320.00
068 Revendication à partir de la 11ème	EURO	15.00	10.00	150.00
Total à acquitter	EURO			505.00

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE	
Signé par	Karine BERTHIER



La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

La présente invention concerne un appareil électrique destiné à être connecté à un réseau comportant au moins un appareil gardien. Elle concerne également un système antivol comportant un réseau auquel est connecté un appareil gardien. Elle concerne enfin un procédé d'appariement d'un premier et d'un second appareils, le premier appareil étant appelé appareil gardien.

On connaît déjà dans l'état de la technique un tel appareil électrique destiné à être connecté à un réseau comportant un appareil gardien. Ce dernier est configuré de façon à empêcher le fonctionnement de l'appareil électrique en cas de vol.

Par exemple, dans le document WO 98/04967, un appareil électrique muni d'un dispositif de protection peut fonctionner uniquement s'il est relié à un appareil gardien autorisant son fonctionnement. L'appareil gardien gère, dans une base de données associée, une liste d'appareils électriques identifiés par un code d'identification unique et comporte des moyens d'autorisation de fonctionnement des appareils enregistrés sur la liste. Généralement, l'appareil gardien est fixé, caché, voire distant, de façon à ce que des voleurs éventuels ne puissent dérober que les appareils électriques connectés à cet appareil gardien. Par conséquent, les voleurs ne possèdent pas l'appareil gardien autorisant le fonctionnement de ces appareils volés et ne peuvent pas utiliser ou revendre ces appareils.

L'inconvénient d'un tel système est que l'autorisation de fonctionnement de l'appareil électrique est gérée par l'appareil gardien. L'appareil gardien gère par ailleurs l'autorisation de fonctionnement de tous les autres appareils de la liste. Cette gestion peut devenir lourde et difficile dans le cas où beaucoup d'appareils électriques sont reliés à l'appareil gardien.

L'invention vise à remédier à cet inconvénient en fournissant un appareil électrique pouvant être protégé contre le vol sans pour autant nécessiter la gestion d'une liste d'appareils électriques par l'appareil gardien auquel il est associé.

A cet effet, l'invention a pour objet un appareil électrique destiné à être connecté à un réseau comportant au moins un appareil gardien, caractérisé en ce qu'il comporte des moyens de configuration pour autoriser son fonctionnement en présence dudit appareil gardien, des moyens d'identification d'au moins un appareil gardien lorsque l'appareil électrique est connecté à un réseau quelconque comportant un tel appareil gardien, et des moyens d'inhibition de l'appareil électrique si l'appareil gardien identifié ne correspond pas à l'appareil gardien pour lequel il a été configuré ou si ledit réseau quelconque ne comporte pas d'appareil gardien.

Un appareil électrique suivant l'invention peut en outre comporter l'une ou plusieurs des caractéristiques suivantes :

- il comporte des moyens de stockage, et les moyens de configuration sont adaptés pour l'enregistrement d'un identifiant public de l'appareil gardien pour lequel l'appareil électrique est configuré, dans les moyens de stockage ;
- les moyens d'identification comportent des moyens d'interrogation d'un appareil gardien quelconque pour connaître son identifiant public ;
- les moyens d'identification comportent des moyens d'authentification de l'appareil gardien pour lequel il a été configuré ;
- les moyens d'authentification mettent en œuvre un procédé de challenge à transfert de connaissance nul ;
- l'appareil électrique est dans un état choisi parmi l'un des éléments de l'ensemble constitué d'un état vierge, d'un état configuré pour fonctionner en présence d'au moins un appareil gardien et d'un état bloqué, l'état configuré étant obtenu après activation des moyens de configuration et l'état bloqué étant obtenu après activation des moyens d'inhibition ; et
- l'appareil électrique fonctionne uniquement lorsqu'il est dans l'état configuré.

L'invention a également pour objet un système antivol comportant au moins un réseau et au moins un appareil gardien connecté au réseau et comportant un identifiant public, caractérisé en ce qu'il comporte au moins un appareil électrique tel que décrit précédemment.

Un système antivol selon l'invention peut en outre comporter l'une ou plusieurs des revendications suivantes :

- l'appareil gardien comporte des moyens sécurisés de stockage d'un identifiant secret à partir duquel l'identifiant public est généré ; et
- le réseau est choisi parmi l'un des éléments de l'ensemble constitué d'un réseau électrique, un réseau de transmission numérique et un réseau de télécommunications.

L'invention a enfin pour objet un procédé d'appariement d'un premier et d'un second appareils, le second appareil étant destiné à être connecté à un réseau auquel est connecté le premier appareil dit "appareil gardien", caractérisé en ce qu'il comporte une étape de configuration du second appareil pour autoriser son fonctionnement uniquement en présence de l'appareil gardien.

Un procédé d'appariement suivant l'invention peut en outre comporter l'une ou plusieurs des caractéristiques suivantes :

- lors de la configuration du second appareil, on enregistre, dans des moyens de stockage de celui-ci, un identifiant public de l'appareil gardien.

- le second appareil est dans un état choisi parmi l'un des éléments de l'ensemble constitué d'un état vierge, d'un état configuré pour fonctionner en présence d'au moins un appareil gardien et d'un état bloqué, et en ce que l'étape de configuration comporte un changement d'état du second appareil, de l'état vierge à l'état configuré ;

- le procédé comporte une étape d'inhibition du second appareil lorsque celui-ci est connecté à un appareil gardien pour lequel il n'a pas été configuré, cette étape d'inhibition comportant un changement d'état du second appareil, de l'état configuré à l'état bloqué ;

- le procédé comporte une étape d'identification d'un appareil gardien connecté à un réseau, lorsque le second appareil est connecté à ce réseau ;

- l'étape d'identification est déclenchée par l'un des événements déclenchant de l'ensemble d'événements constitué d'une connexion du second appareil au réseau, une mise en marche du second appareil et un programme d'identification régulière ou aléatoire ;

- l'étape d'identification comporte l'authentification de l'appareil gardien ;

- l'authentification est réalisée par l'utilisation d'un procédé de challenge à transfert de connaissance nul ;

- l'appareil gardien comportant des moyens sécurisés de stockage d'un identifiant secret à partir duquel un identifiant public est généré, l'identification comporte une étape d'interrogation de l'appareil gardien pour connaître son identifiant public et l'authentification comporte une séquence d'étapes lors de laquelle l'appareil gardien prouve à l'appareil électrique qu'il connaît l'identifiant secret à l'aide du procédé de challenge à transfert de connaissance nul ; et

- si l'étape d'identification conclut à la présence sur le réseau de l'appareil gardien pour lequel le second appareil a été configuré alors que le second appareil est à l'état bloqué, elle est suivie d'un changement d'état du second appareil de l'état bloqué à l'état configuré.

L'invention sera mieux comprise à l'aide de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant aux dessins annexés sur lesquels :

- la figure 1 représente schématiquement un système antivol selon l'invention ;

- la figure 2 représente le diagramme fonctionnel d'un procédé de changement d'états d'un appareil électrique selon l'invention ; et
- la figure 3 représente le diagramme fonctionnel d'un procédé d'appariement d'un appareil électrique à un appareil gardien selon l'invention.

On a représenté sur la figure 1 un réseau local 10 tel qu'un réseau de distribution d'énergie électrique, un réseau de transmission numérique ou encore un réseau de télécommunications. Il peut s'agir d'un réseau filaire ou sans fil. A ce réseau local 10 sont connectés un appareil gardien 12 et des appareils électriques 14.

L'appareil gardien 12 peut être caché ou fixé à un support de façon à ce qu'on puisse difficilement le voler. Il comprend des moyens de calcul 16 tels qu' un processeur sécurisé et une interface réseau 18. L'appareil gardien 12 stocke en mémoire (non représentée sur la figure) un très grand nombre secret S et un nombre V, appelé par la suite identifiant public de l'appareil gardien 12. S et V vérifient l'équation suivante :

$$S = \sqrt{V} \bmod n,$$

où n est un entier dont la factorisation est secrète, par exemple en étant le produit de deux très grands nombres premiers tenus secrets.

On vérifie aisément que si $S = \sqrt{V} \bmod n$ alors $S^2 = V \bmod n$.

L'appareil gardien 12 stocke également une signature SigV de l'identifiant public V calculée par une autorité de contrôle, à l'aide d'une clé publique K.

V et n sont des valeurs publiques, c'est à dire connues de l'appareil gardien 12, mais qui peuvent aussi être communiquées aux appareils électriques 14. Alors que la valeur n est stockée dans les appareils électriques 14 à la construction, la valeur V est transmise aux appareils électriques 14 lors de leur configuration.

Les appareils électriques 14 sont par exemple des appareils électroménagers, audiovisuels, informatiques ou tout autre appareil que l'on désire protéger contre le vol et adapté pour être connecté au réseau 10. Chaque appareil électrique 14 comporte des moyens de stockage 20, tels qu'une mémoire non volatile, des moyens de calcul 22 tels qu'un processeur et une interface réseau 24 similaire à l'interface réseau 18 de l'appareil gardien 12.

Les moyens de calcul 22 comportent des moyens 26 de configuration de chaque appareil électrique 14, des moyens 28 d'identification d'appareils gardiens et des moyens 30 d'inhibition de chaque appareil

électrique 14. Ces moyens 26, 28 et 30 sont avantageusement des moyens logiciels programmés de façon classique dans le processeur 22 de chaque appareil électrique 14.

Chaque appareil électrique 14 stocke dans sa mémoire 20 le nombre n et la clé publique K issue de l'autorité de contrôle ayant calculé la signature SigV. Cette clé permet de vérifier la signature SigV en fonction de la valeur de V.

Dans le mode de réalisation représenté, l'invention vise à restreindre l'usage de chaque appareil 14 au réseau local 10, c'est à dire que chaque appareil électrique 14 ne peut fonctionner que s'il est relié à l'appareil gardien 12. Dans ce cas, la mémoire 20 de chaque appareil 14 stocke uniquement l'identifiant public V de l'appareil gardien 12, en plus de n et K.

Dans un autre mode de réalisation, l'usage de chaque appareil électrique 14 peut être restreint à plusieurs réseaux locaux comportant chacun un appareil gardien. Chaque appareil électrique 14 peut donc être associé à plusieurs appareils gardiens. Dans ce cas, la mémoire 20 de chaque appareil 14 stocke l'identifiant public V de chaque appareil gardien auquel il est associé.

L'appareil électrique 14 peut se trouver dans trois états fondamentaux, représentés sur la figure 2 : un état vierge 32, un état configuré 34 et un état bloqué 36.

L'état vierge 32 correspond à un état dans lequel la mémoire 20 de l'appareil électrique 14 ne stocke aucun identifiant public d'appareil gardien.

L'état configuré 34 correspond à un état dans lequel l'appareil électrique 14 stocke dans sa mémoire 20 l'identifiant public V de l'appareil gardien 12. L'appareil électrique 14 peut alors fonctionner uniquement en présence de l'appareil gardien 12, c'est à dire lorsque l'appareil 14 est connecté à un réseau auquel est aussi connecté l'appareil gardien 12.

Dans un autre mode de réalisation, l'état configuré correspond à un état dans lequel la mémoire 20 de chaque appareil 14 stocke des identifiants publics V de plusieurs appareils gardiens prédéterminés. L'appareil électrique 14 peut alors fonctionner s'il est connecté à l'un des appareils gardiens dont il contient l'identifiant public V.

L'état bloqué 36 correspond à un état dans lequel l'appareil électrique, bien qu'ayant été configuré, ne peut pas fonctionner car il est relié à un appareil gardien pour lequel il n'a pas été configuré, c'est à dire dont il ne connaît pas l'identifiant public V, ou bien il n'est relié à aucun appareil gardien.

Dans la suite, l'état de l'appareil électrique 14 sera défini par une variable e, stockée dans sa mémoire 20, à laquelle on donne la valeur 0 si

l'appareil électrique 14 est à l'état vierge 32, la valeur 1 s'il est à l'état configuré 34 et la valeur 2 s'il est à l'état bloqué 36.

On peut passer de l'état vierge 32 à l'état configuré 34 par une étape de configuration 38 au cours de laquelle on enregistre dans la mémoire 20 de l'appareil électrique 14 l'identifiant public V de l'appareil gardien 12 afin que l'appareil électrique 14 identifie l'appareil gardien 12 et puisse fonctionner en sa présence.

Dans le mode de réalisation décrit, l'étape de configuration 38 est automatique, par exemple lors de la connexion de l'appareil électrique 14 au réseau 10, ou lors de la mise en marche de l'appareil électrique 14, pour la première fois.

En variante, l'étape de configuration 38 peut être déclenchée manuellement par l'utilisateur, par exemple grâce à la saisie d'un code secret, à l'utilisation d'une clé physique ou électronique, ou à une authentification de l'utilisateur par des moyens de biométrie comme la reconnaissance d'empreintes digitales ou vocales.

On passe de l'état configuré 34 à l'état bloqué 36 par une étape automatique d'inhibition 40 déclenchée lorsque l'appareil électrique 14 est relié à un appareil gardien autre que l'appareil gardien 12 pour lequel il a été configuré, c'est à dire un appareil gardien dont l'identifiant public V n'est pas stocké dans la mémoire 20 de l'appareil électrique 14, ou lorsqu'il n'est relié à aucun appareil gardien.

On passe de l'état bloqué 36 à l'état configuré 34 par une étape automatique de déblocage 42. Cette étape est déclenchée lorsque l'appareil électrique 14 bloqué est de nouveau relié à l'appareil gardien 12 dont il contient l'identifiant public V. L'appareil électrique 14 se retrouve alors à l'état configuré 34, après la mise en œuvre d'un test de type challenge à transfert de connaissance nulle qui sera décrit ci-dessous, en référence à la figure 3.

En variante, l'étape de déblocage 42 peut être déclenchée manuellement, par exemple lors de la saisie d'un mot de passe, lors de l'utilisation d'une clé physique ou électronique ou lors de l'authentification de l'utilisateur par des moyens de biométrie.

Enfin, on passe de l'état configuré 34 à l'état vierge 32 par une étape de réinitialisation 44 au cours de laquelle un utilisateur autorisé efface tous les identifiants publics d'appareils gardiens stockés dans la mémoire 20 de l'appareil électrique 14.

Le procédé d'appariement de l'appareil électrique 14 à un appareil gardien quelconque 46 est décrit sur le diagramme fonctionnel de la figure 3.

Ce procédé d'appariement comporte une première étape d'initialisation 48 constituée d'un événement déclenchant tel que la mise en marche de l'appareil électrique 14, sa connexion à un réseau, ou un top d'horloge périodique. Dans tous les cas, on suppose que l'appareil électrique est connecté à un réseau auquel est également connecté l'appareil gardien 46.

Lors de l'étape 50 suivante, l'appareil électrique 14 envoie une commande demandant à l'appareil gardien 46 présent sur le réseau de s'identifier.

Ensuite, lors d'une étape 52, l'appareil gardien 46 transmet à l'appareil électrique 14 son identifiant public V ainsi que sa signature SigV.

A la suite de cette étape 52, un test 54 est effectué par l'appareil électrique 14. Ce test consiste à vérifier la signature SigV à l'aide de l'identifiant public V envoyé par l'appareil gardien 46 et de la clé publique K stockée dans l'appareil électrique 14.

Si le résultat du test 54 est négatif, c'est à dire si la signature SigV ne correspond pas à l'identifiant transmis V, le procédé est reporté à l'étape d'initialisation 48.

Si le résultat du test 54 est positif, un test 56 est effectué sur la variable e stockée dans la mémoire 20 de l'appareil électrique 14.

Si la variable e vaut 0, c'est à dire si l'appareil électrique 14 est à l'état vierge 32, on passe à une étape 58 au cours de laquelle l'appareil 14 stocke l'identifiant public V dans sa mémoire 20. L'étape 58 est suivie de l'étape de configuration 38 décrite précédemment. Au cours de cette étape, la variable e prend la valeur 1 et l'appareil électrique 14 se trouve alors dans l'état configuré 34. Le procédé est ensuite reporté à l'étape d'initialisation 48.

Si à l'étape 56 la variable e vaut 1 ou 2, on passe à une étape de test 60 au cours de laquelle l'appareil électrique 14 compare l'identifiant public V envoyé par l'appareil gardien 46 à l'identifiant public V_0 stocké dans sa mémoire 20.

Si le résultat du test 60 est négatif, l'appareil électrique 14 effectue un test 61 sur la variable e. Si e vaut 2, l'appareil étant déjà inhibé, on passe à l'étape d'initialisation 48. Sinon, e valant 1, on passe à l'étape d'inhibition 40 décrite précédemment. Au cours de cette étape la variable e prend la valeur 2, c'est à dire que l'appareil électrique 14 se trouve dans l'état bloqué 36. Le procédé est ensuite reporté à l'étape d'initialisation 48.

Si le résultat du test 60 est positif, on passe à une étape 62 au cours de laquelle l'appareil gardien 46 déclenche un procédé de challenge à transfert

de connaissance nulle, en générant tout d'abord un nombre aléatoire r. Ce procédé fait l'objet des étapes 62 à 86.

A la suite de cette étape 62, on passe à une étape 64 lors de laquelle l'appareil gardien 46 choisit un gage G qui est un nombre pris aléatoirement parmi les deux nombres r^2 et $r.S$ où S est le nombre secret de l'appareil gardien 46. Il transmet ce gage G à l'appareil électrique 14 sans l'informer de son choix.

Lors de l'étape 66 suivante, l'appareil électrique 14 affecte aléatoirement une valeur A ou B à un challenge C. Il envoie ensuite ce challenge C à l'appareil gardien 46.

A la suite de cette étape 66, l'appareil gardien 46 effectue un test 68 sur le challenge C.

Si le test 68 révèle que le challenge C vaut A, on passe à une étape 70 au cours de laquelle l'appareil gardien 46 affecte la valeur r^2 à A et renvoie A à l'appareil électrique 14.

A la suite de cette étape 70, l'appareil électrique 14 effectue un test 72 de vérification de la valeur du gage G.

On sait que, à la suite de l'étape 64, le gage G vaut r^2 ou $r.S$. Comme $A = r^2$, nous avons deux possibilités : soit $G = A$ (dans le cas où $G = r^2$), soit $r^2.S^2 = A.V \bmod n$ (dans le cas où $G = rS$). En effet, dans ce dernier cas, si l'identifiant public V correspond à l'appareil gardien 46, c'est à dire si $S^2 = V \bmod n$, alors $r^2.S^2 = A.V \bmod n$. Donc si V est bien l'identifiant de l'appareil gardien 46, $G = A$ ou $G^2 = A.V \bmod n$.

Si le test 72 est positif c'est à dire si $G = A$ ou si $G^2 = A.V \bmod n$, on passe à une étape 74 lors de laquelle on donne la valeur 1 à e, c'est à dire que l'appareil électrique est mis à l'état configuré 34.

A la suite de cette étape 74, on passe à une étape 76 de surveillance d'événements déclenchant. Au cours de cette étape 76, dès qu'un événement déclenchant, faisant partie d'un ensemble d'événements déclenchant prédéterminés, est détecté, on passe à l'étape 62. Ces événements déclenchant sont par exemple les mêmes que ceux de l'étape 48.

Si le test 72 est négatif, c'est à dire si $G \neq A$ et $G^2 \neq A.V \bmod n$, on passe à une étape 78 lors de laquelle on donne la valeur 2 à e, c'est à dire que l'appareil électrique est mis à l'état bloqué 36.

A la suite de cette étape 78 on passe à l'étape 76 de surveillance d'événements déclenchant.

Si le test 68 révèle que le challenge C vaut B on passe à une étape 80 au cours de laquelle l'appareil gardien 46 affecte à B la valeur $r.S$ et envoie B à l'appareil électrique 14.

A la suite de cette étape 80, l'appareil électrique 14 effectue un test 82 de vérification de la valeur du gage G.

On sait que, à la suite de l'étape 64, le gage G vaut r^2 ou $r.S$. Comme $B = r.S$, nous avons deux possibilités : soit $G = B$ (dans le cas où $G = rS$), soit $r^2.S^2 = G.V \bmod n$ (dans le cas où $G = r^2$). En effet, dans ce dernier cas, si l'identifiant public V correspond à l'appareil gardien 46, c'est à dire si $S^2 = V \bmod n$, alors $r^2.S^2 = G.V \bmod n$. Donc si V est bien l'identifiant de l'appareil gardien 46, $G = B$ ou $B^2 = G.V \bmod n$.

Si le test 82 est positif c'est à dire si $G = B$ ou si $B^2 = G.V \bmod n$, on passe à une étape 84 lors de laquelle on donne la valeur 1 à e, c'est à dire que l'appareil électrique est mis à l'état configuré 34.

A la suite de cette étape 84, on passe à l'étape 76 de surveillance d'événements déclenchant.

Si le test 82 est négatif, c'est à dire si $G \neq B$ et $B^2 \neq G.V \bmod n$, on passe à une étape 86 lors de laquelle on donne la valeur 2 à e, c'est à dire que l'appareil électrique est mis à l'état bloqué 36.

A la suite de cette étape 78 on passe à l'étape 76 de surveillance d'événements déclenchant.

Parmi les avantages de l'invention, on notera que celle-ci permet à chaque appareil électrique de ne fonctionner qu'en présence de l'appareil gardien pour lequel il a été configuré, sans que pour autant le gardien ait à gérer une liste d'appareils autorisés.

On notera aussi que celle-ci permet un test antivol automatique, sans nécessiter l'intervention d'une autorité centrale.

Enfin, aucune information secrète n'est stockée dans les appareils électriques 14 grâce à l'utilisation d'un procédé de challenge à transfert de connaissance nul pour l'authentification.

REVENDICATIONS

1. Appareil électrique (14) destiné à être connecté à un réseau prédéterminé (10) comportant au moins un appareil gardien (12), caractérisé en ce qu'il comporte des moyens de configuration (26) pour autoriser son fonctionnement en présence dudit appareil gardien (12), des moyens (28) d'identification d'au moins un appareil gardien lorsque l'appareil électrique est connecté à un réseau quelconque comportant un tel appareil gardien, et des moyens (30) d'inhibition de l'appareil électrique (14) si l'appareil gardien identifié ne correspond pas à l'appareil gardien (12) pour lequel il a été configuré ou si ledit réseau quelconque ne comporte pas d'appareil gardien.

2. Appareil électrique (14) selon la revendication 1, caractérisé en ce qu'il comporte des moyens de stockage (20), et en ce que les moyens de configuration (26) sont adaptés pour l'enregistrement d'un identifiant public (V) de l'appareil gardien (12) pour lequel l'appareil électrique est configuré, dans les moyens de stockage (20).

3. Appareil électrique (14) selon la revendication 2, caractérisé en ce que les moyens d'identification (28) comportent des moyens d'interrogation d'un appareil gardien quelconque pour connaître son identifiant public (V).

4. Appareil électrique (14) selon l'une quelconque des revendications 1 à 3, caractérisé en ce que les moyens d'identification (28) comportent des moyens d'authentification de l'appareil gardien (12) pour lequel il a été configuré.

5. Appareil électrique (14) selon la revendication 4, caractérisé en ce que les moyens d'authentification mettent en œuvre un procédé de challenge à transfert de connaissance nul.

6. Appareil électrique (14) selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il est dans un état choisi parmi l'un des éléments de l'ensemble constitué d'un état vierge (32), d'un état (34) configuré pour fonctionner en présence d'au moins un appareil gardien (14) et d'un état bloqué (36), l'état configuré (34) étant obtenu après activation des moyens de

configuration (26) et l'état bloqué (36) étant obtenu après activation des moyens d'inhibition (30).

7. Appareil électrique (14) selon la revendication 6, caractérisé en ce qu'il fonctionne uniquement lorsqu'il est dans l'état configuré (34).

8. Système antivol comportant au moins un réseau (10) et au moins un appareil gardien (12) connecté au réseau et comportant un identifiant public (V), caractérisé en ce qu'il comporte au moins un appareil électrique (14) selon l'une quelconque des revendications 1 à 7.

9. Système antivol selon la revendication 8, caractérisé en ce que l'appareil gardien (12) comporte des moyens sécurisés (16) de stockage d'un identifiant secret (S) à partir duquel l'identifiant public (V) est généré.

10. Système antivol selon la revendication 8 ou 9, caractérisé en ce que le réseau (10) est choisi parmi l'un des éléments de l'ensemble constitué d'un réseau électrique, un réseau de transmission numérique et un réseau de télécommunications.

11. Procédé d'appariement d'un premier (12) et d'un second (14) appareils, le second appareil (14) étant destiné à être connecté à un réseau (10) auquel est connecté le premier appareil (12) dit "appareil gardien", caractérisé en ce qu'il comporte une étape de configuration du second appareil (14) pour autoriser son fonctionnement uniquement en présence de l'appareil gardien (12).

12. Procédé d'appariement selon la revendication 11, caractérisé en ce que lors de la configuration du second appareil (14), on enregistre, dans des moyens de stockage (20) de celui-ci, un identifiant public (V) de l'appareil gardien.

13. Procédé d'appariement selon la revendication 11 ou 12, caractérisé en ce que le second appareil (14) est dans un état choisi parmi l'un des éléments de l'ensemble constitué d'un état vierge (32), d'un état (34) configuré pour fonctionner en présence d'au moins un appareil gardien (14) et d'un état bloqué (36), et en ce que l'étape de configuration comporte un

changement d'état du second appareil (14), de l'état vierge (32) à l'état configuré (34).

14 Procédé d'appariement selon la revendication 13, caractérisé en ce qu'il comporte une étape d'inhibition du second appareil (14) lorsque celui-ci est connecté à un appareil gardien pour lequel il n'a pas été configuré, cette étape d'inhibition comportant un changement d'état du second appareil (14), de l'état configuré (34) à l'état bloqué (36).

15. Procédé d'appariement selon la revendication 13 ou 14, caractérisé en ce qu'il comporte une étape d'identification d'un appareil gardien connecté à un réseau, lorsque le second appareil (14) est connecté à ce réseau.

16. Procédé d'appariement selon la revendication 15, caractérisé en ce que l'étape d'identification est déclenchée par l'un des événements déclenchant de l'ensemble d'événements constitué d'une connexion du second appareil (14) au réseau, une mise en marche du second appareil et un programme d'identification régulière ou aléatoire.

17. Procédé d'appariement selon la revendication 15 ou 16, caractérisé en ce que l'étape d'identification comporte l'authentification de l'appareil gardien.

18. Procédé d'appariement selon la revendication 17, caractérisé en ce que l'étape d'authentification est réalisée par l'utilisation d'un procédé de challenge à transfert de connaissance nul.

19. Procédé d'appariement selon la revendication 18, caractérisé en ce que, l'appareil gardien (12) comportant des moyens sécurisés (16) de stockage d'un identifiant secret (S) à partir duquel un identifiant public (V) est généré, l'identification comporte une étape d'interrogation de l'appareil gardien pour connaître son identifiant public (V) et l'authentification comporte une séquence d'étapes lors de laquelle l'appareil gardien (12) prouve à l'appareil électrique (14) qu'il connaît l'identifiant secret (S) à l'aide du procédé de challenge à transfert de connaissance nul.

20. Procédé d'appariement selon l'une quelconque des revendications 15 à 19, caractérisé en ce que si l'étape d'identification conclut à la présence sur le réseau de l'appareil gardien (12) pour lequel le second appareil (14) a été configuré alors que le second appareil est à l'état bloqué, elle est suivie d'un changement d'état du second appareil (14) de l'état bloqué (36) à l'état configuré (34).

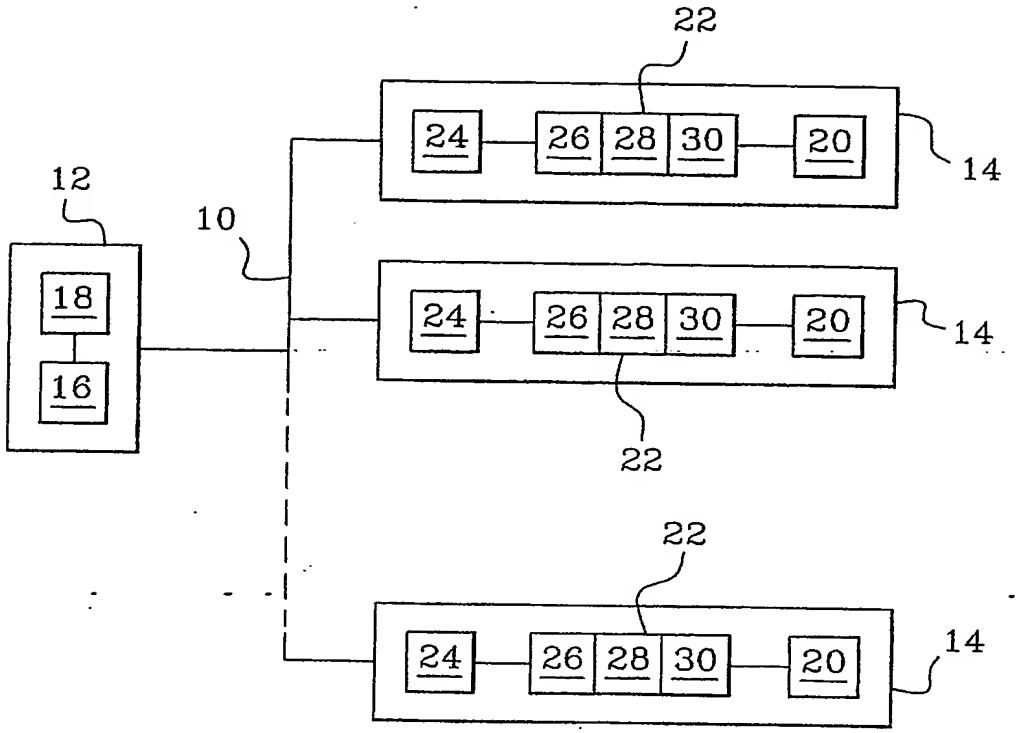

22
24
26
28
30
20
14
12
10
18
16
24
26
28
30
20
14
22
22
24
26
28
30
20
14

Fig. 1

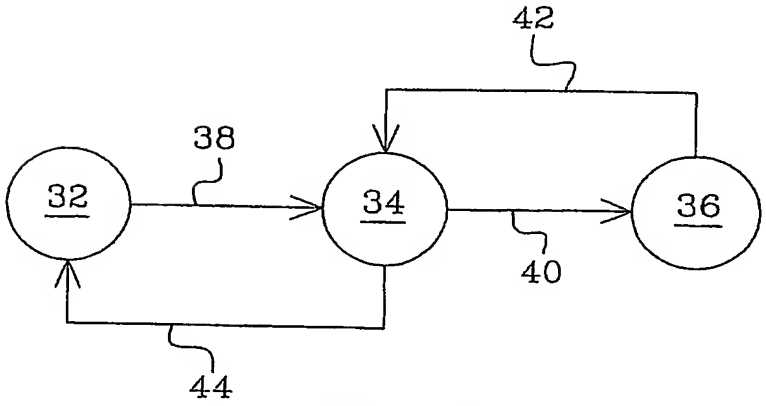
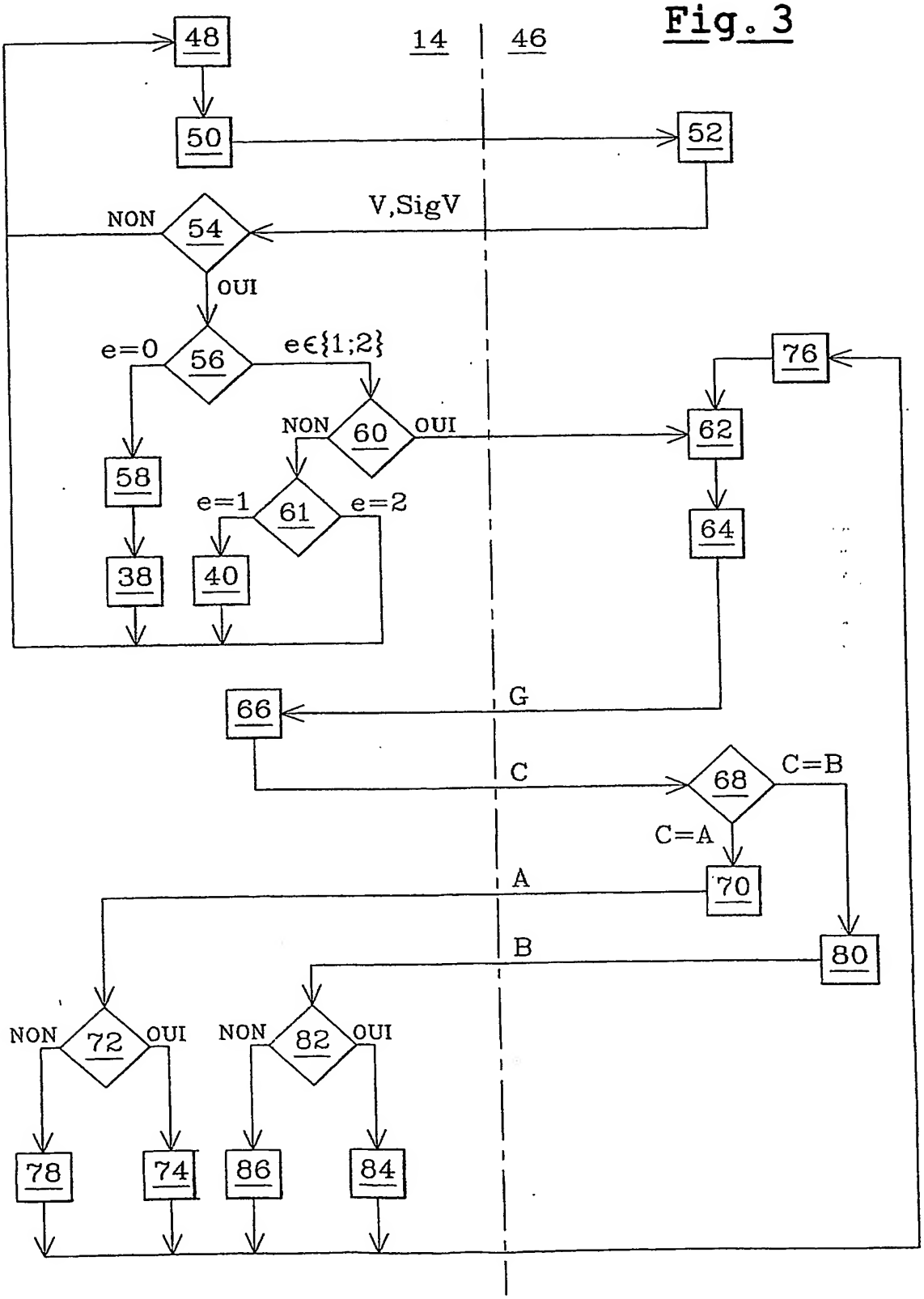

42
38
32
34
36
40
44

Fig. 2

Fig. 3


48
14
46
50
52
NON
54
V,SigV
OUI
e=0
56
e∈{1;2}
76
NON
60
OUI
62
58
e=1
61
e=2
64
38
40
66
G
C
68
C=B
C=A
70
A
B
80
NON
72
OUI
NON
82
OUI
78
74
86
84

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

Désignation de l'inventeur

Vos références pour ce dossier	PF020104
N°D'ENREGISTREMENT NATIONAL	0210430
TITRE DE L'INVENTION	
	APPAREIL ELECTRIQUE SECURISE CONTRE LE VOL, SYSTEME ANTIVOL COMPORTANT UN TEL APPAREIL ET PROCEDE D'APPARIEMENT D'APPAREILS ELECTRIQUES
LE(S) DEMANDEUR(S) OU LE(S) MANDATAIRE(S):	Karine BERTHIER

DESIGNE(NT) EN TANT QU'INVENTEUR(S):	
Inventeur 1	
Nom	CHEVREAU
Prénoms	Sylvain
Rue	9 Square Roi Arthur
Code postal et ville	35000 RENNES
Société d'appartenance	
Inventeur 2	
Nom	DIEHL
Prénoms	Eric
Rue	La Buzardière
Code postal et ville	35340 Liffré
Société d'appartenance	
Inventeur 3	
Nom	FURON
Prénoms	Teddy
Rue	13 rue de la Santé
Code postal et ville	35000 RENNES
Société d'appartenance	

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE	
Signé par:	Karine BERTHIER
Date	20 août 2002

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Référence EASY : 67592